SHIELD FORCE

PROTECCIÓN BANCA MÓVIL

Una nueva amenaza

La banca móvil, el pago móvil, la billetera móvil y proveedores FinTech que entregan servicios en Aplicaciones Móviles de Android a sus clientes, ahora tienen que lidiar con un nuevo malware de recolección de datos. Esto fue descubierto el 30/04/20 por el equipo de investigación Nocturnus en Cybereason, el malware se conoce como "**EventBot**".

Si desea saber si su aplicación de banca móvil, pago móvil, billetera electrónica o cripto moneda es vulnerable a EventBot, u otro malware móvil, escriba a:

ventas@shieldforce.mx

Protección a los clientes de la Banca Móvil

Eventbot

Es un Malware oculto dentro de una aplicación móvil aparentemente válida, que recolecta datos desprotegidos de aplicaciones víctimas en el dispositivo Android. TechCrunch informa que **EventBot** a menudo se hace pasar por una aplicación legítima de Android, como Adobe Flash o Microsoft Word para Android. Una vez instalado, **EventBot** recolecta datos, ampliando los permisos y obteniendo acceso a las opciones de accesibilidad en el sistema operativo Android.

EventBot es de cuidado por tres razones. Primero, se puede ocultar en una versión modificada de una aplicación aparentemente legítima. Actualmente, se esconde en aplicaciones diseñadas para el trabajo. En segundo lugar, **EventBot** apunta a datos desprotegidos en banca móvil, pago móvil, billetera móvil y aplicaciones similares. ZDnet advierte que **EventBot** está dirigido específicamente a la banca móvil, aplicaciones móviles y billeteras de criptomonedas en Europa y Estados Unidos en busca de credenciales de usuario, contraseñas de un solo uso (OTP) y detalles de la cuenta. **EventBot** está diseñado para robar nombres de usuario, contraseñas e interceptar códigos de autenticación de dos factores enviados por estas aplicaciones como mensajes de texto. Tercero, está evolucionando rápidamente y es primordial emplear medidas de seguridad para protegerse contra este malware.

¿Como Trabaja?

El propósito principal de **EventBot** es la recolección de datos. Recopila y extrae datos no protegidos de las aplicaciones móviles específicas. Lo que es muy revelador sobre **EventBot** es su capacidad para realizar su intención maliciosa utilizando métodos estándar disponibles a través del sistema operativo Android. Por ejemplo, el usuario instala la aplicación modificada con el malware **EventBot** en su interior a través de tiendas alternativas de aplicaciones legítimas y apócrifas. No es tan difícil para **EventBot** usar PackageManage (o un método similar) para obtener un inventario de todas las aplicaciones móviles en el dispositivo Android. Con el inventario en mano, **EventBot** podría comparar el inventario de la aplicación con una lista objetivo de BundleID para determinadas aplicaciones bancarias, de pago y de billetera que busca explotar.

A partir de ahí, al extraer los datos no protegidos de las aplicaciones, incluidos nombres de usuario y contraseñas, claves y secretos de la API, y más, el malware aprovecha de manera inteligente los métodos estándar para extraer datos y obtener permisos. Por ejemplo, presenta una pantalla al usuario que le pide que otorgue más permisos, lo que le permite interceptar mensajes de texto entrantes.

No hace falta mucha imaginación para darse cuenta de que un mal actor con un nombre de usuario y contraseña recopilados de una aplicación móvil desprotegida ahora puede realizar todas las formas de fraude, robo de identidad y acceder al mismo servicio en línea utilizando las credenciales robadas. Con acceso al SMS del usuario, no tomaría mucho realizar una toma de control de la cuenta bancaria, de pago o criptográfica de una persona en cualquier navegador o teléfono en el mundo.

¿Por que es tan importante?

Cybereason descubrió que **EventBot** apunta a usuarios de más de 200 aplicaciones financieras, incluidos servicios bancarios, servicios de transferencia de dinero y billeteras de criptomonedas. Los objetivos incluyen aplicaciones como Paypal Business, Revolut, Barclays, UniCredit, CapitalOne UK, HSBC UK, Santander UK, TransferWise, Coinbase, paysafecard y muchos más. En Shield Force entendemos este problema y por ello ofrecemos el servicio **Appdome Mobile Trust.**

Appdome Mobile Trust

Protección modular para cualquier aplicación móvil. Es un servicio en la nube siempre activo.

No codificas, no instalas software o hardware.

Total Data Encryption

Protección Datos Móviles

¿Que protege?

- Dato en Reposo
- Dato en el App
- Dato en Memoria
- Cadenas de Datos
- Datos en Preferencias
- Datos Secretos
- FIPS 140-2 Cryptography

Trusted Communication

Refuerzo Antibot F5

¿Que Provee?

- Protección Anti-Bot F5
- Integración Silverline F5
- Sesiones Seguras (TLS)
- Certificate Pinning
- Protección SecureAPI™
- Refuerzo Digestión SHA256

Mobile Integrity

Verificación y Prevención

¿Que Provee?

- Protección Jailbreak/Root
- Bloqueo Keylogger
- Prevención de Compartir Pantalla
- Privacidad de Pantalla
- Detección de Dispositivos Prohibidos (Banned)

TotalCode Ofuscation

Ofuscación de Código Móvil

¿Que protege?

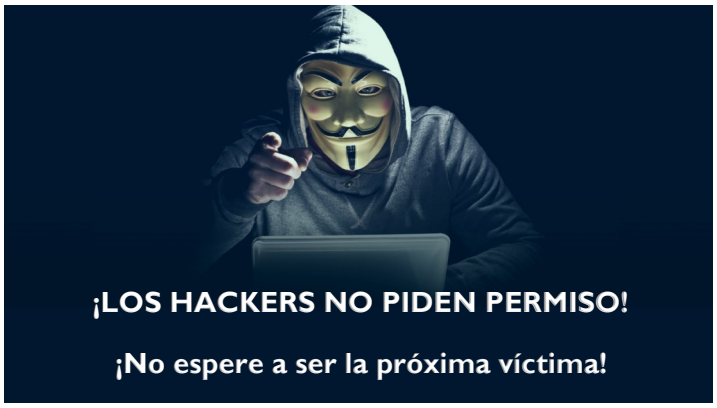
- Lógica de Apps Móviles
- Código Nativo y no nativo
- Previene la Imitación de Apps
- Reduce la exposición al Hacking
- Protege Secretos de App
- Cualquier SDK

One Shield

Fortalecimiento de Apps

¿Que Detiene?

- Manipulación
- Ingeniería en Reversa
- Depuración Maliciosa
- Alteración de Aplicaciónes
- Infiltración de Apps
- Prevención de Emulador



Contáctenos

Le ofrecemos una prueba de concepto del servicio y evalúe los beneficios de proteger sus aplicaciones móviles.